NAVAL RESEARCH LABORATORY

NAVAL CENTER FOR SPACE TECHNOLOGY

Safety, Reliability and Quality Assurance (SR&QA) Plan
for the
Full-Sky Astrometric Mapping Explorer (FAME)

NCST-D-FM006 **08 December 2000**

Approved By:_____ Date: _____
M. Johnson, Program Manager

Approved By:_____ Date: _____
K. Johnston, Principle Investigator

Concurrence: _____ Date: _____
Cognizant NASA Manager

4555 Overlook Avenue, S.W.
Washington, D.C. 20375-5000

RECORD OF CHANGES

REVISION LETTER	DATE	TITLE OR BRIEF DESCRIPTION	ENTERED BY
—	08 December 2000	Draft Release for SRR	R. Spencer

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 Purpose.

This plan describes the safety and reliability-oriented tasks applicable to the FAME program. This plan also describes the parts, materials, and process controls and procedures. these analysis and control procedures are necessary to assure delivery of a safe and reliable system capable of successfully performing the FAME mission.

2. APPLICABLE DOCUMENTS

The following documents form a part of this document to the extent specified herein.

Military Standards

Number	Title	Paragraph Cited
MIL-STD-883	Test Methods and Procedures for Micro-Electronics	5.2
MIL-STD-975	NASA Standard Electrical, Electronic and Electromechanical (EEE) Parts List	5.2

NCST Manuals

Number	Title	Paragraph Cited
NCST-MCP-001	NCST Manual for Control Procedures Configuration Item Verification, CP-03.03	 5.14
NCST-MMP-001	NCST Manual for Manufacturing Procedures Non-Standard Parts Approval Request, MP-09.01 Development and Control of Standard Processes, MP-11.01	 5.3 5.13
NCST-MQA-001	NCST Manual for Quality Assurance Procedures Nonconforming Material Reports, QA-14.01	 5.11

NCST Documents

Number	Title	Paragraph Cited
NCST-D-FM005	FAME Quality Assurance Plan	5.14
NCST-D-FM010	FAME Safety Implementation Plan	3
NCST-D-FM011	FAME Failure Mode and Effects Analysis	4.3, 4.4
NCST-D-FM012	FAME EEE Parts List	5.8, 5.15
NCST-D-FM013	FAME Materials List	5.8, 5.15
NCST-D-FM015	FAME Space Segment Reliability Analysis	4.1, 4.2.2, 4.4
NCST-D-FMXXX	FAME Radiation Effects Plan	5.7
NCST-TP-FM001	FAME Test Plan	6
SSD-D-002	EEE Parts Control Plan	5.3
SSD-D-008	Failure Reporting, Analysis and Corrective Action Procedure	5.12
SSD-D-210	Worst Case Analysis and Part Derating Guidelines and Criteria	4.2.2, 4.2.3, 5.6

NASA Documents

Number	Title	Paragraph Cited
311-INST-001	Instructions for EEE Parts Selection, Screening, and Qualification	5.2, 5.4

3. SAFETY

NCST shall utilize a disciplined approach to identification, mitigation, and control of the risks and hazards inherent in the design, fabrication, test, processing, launch and on-orbit operations of FAME. These elements, as well as, safety requirements, analyses, verification, organization, training, reviews and mishap reporting are described in the *FAME Safety Implementation Plan*, NCST-D-FM010.

4. RELIABILITY

The purpose of the reliability program is to assure that the inherent reliability of the units and subsystems for the FAME program. The accomplishment of this purpose requires a controlled iterative implementation of the design analysis and review techniques that identify reliability achievement and enhancement potential. The flow diagram depicting the integration of reliability engineering into the design process is illustrated in Figure 4-1. The individual elements of this reliability analysis program as they apply during the conceptual design period and at the subsystem and system levels during detailed design and development are described in the following paragraphs.

4.1 Preliminary Studies and Evaluation.

The reliability analysis effort begins early in the FAME program design process to provide reliability inputs to design concept trade-off studies and identify reliability improvement possibilities when their implementation has no significant cost or schedule impact. These early studies and evaluations include redundancy trade-off evaluations, with emphasis on equipment interfaces and limited redundancy implementations, technology selection support studies, part selection evaluations, preliminary system reliability achievement potential, and a preliminary Spacecraft Single Point Failure Summary (SPFS). During these preliminary studies the analytical techniques described in paragraph 4.2 for the final subsystem analyses are employed to the extent and level of detail practical.

A result of this preliminary analysis, a FAME reliability evaluation report will be initiated. This report, NCST-D-FM015, will be developed in phases and will serve as both a planning document and as a summary evaluation document. The initial release will follow PDR and will identify and define those subsystems and elements on which FMEA's will be performed. It will also identify and define the subsystems for which a worst-case analysis will be performed.

4.2 Subsystem Reliability Analysis.

As subsystem and unit design detail becomes available, but prior to design finalization, the reliability analysis program scope is increased to include part selection evaluations, electrical stress analyses, design margin analyses and tests, detailed failure mode effect and criticality analyses, and reliability predictions. Existing analyses performed on designs that have not been modified are reviewed for adequacy. The analysis techniques employed on subsystems requiring analysis are described in the following paragraphs.

4.2.1 Failure Modes and Effects Analysis (FMEA).

The Failure Modes and Effects Analysis (FMEA) is a comprehensive, systematic evaluation of viable circuit failure modes and their effect on the subsystem under analysis and the ultimate effects on the FAME program system operation. Emphasis is placed on the identification and evaluation of:

1) All credible failure modes at the unit/functional interfaces and at all internal redundancy interfaces that could affect the redundancy implementation.
2) The effects of all credible failure modes induced from external test equipment to flight hardware.
3) The identification of functions which are not or can not be monitored or tested during preflight and flight conditions.
4) The identification of FAME program system level single point failures.

Criticality category definitions are defined for the FAME program system and the FAME program subsystems in accordance with Table 4-1. These system and subsystem level definitions will ensure that all the FMEA's will use the same criticality categories which will enable the integration of the subsystem level FMEA's into a FAME program system level FMEA for the identification of single point failures.

Item criticality's are calculated as a function of the probability of failure and the mission time to provide a quantitative means of evaluating the severity of the failure mode as a function on the probability of occurrence during the mission lifetime and the criticality category.

The detailed interface FMEA results are recorded on a FMEA worksheet. Figure 4-2 illustrates the unit/functional interface and internal redundancy interface worksheet format with sample entries. The content of each column of

this worksheet and the applicable ground rules and/or assumptions associated with the data developed in each column are summarized in Table 4-2

Figure 4–1.

Flow Diagram Depicting the Integration of Reliability Engineering into the Design Process

Table 4-1. FMEA Criticality Categories

Critical Category	Failure Effect
I	Loss of entire subsystem function.
II	Loss of redundancy within the subsystem.
III	Partial loss of redundancy of subsystem function, e.g., loss of a single functional circuit in a redundant logic section.
IV	No effect on subsystem or more than one success path remains.

Table 4-2. FAME Program FMEA Worksheet Content

FMEA Worksheet Column	Content Description, Ground Rules and/or Assumptions
1	FAILURE PART/SUBSYSTEM/COMPONENT: This column is used to identify the part/subsystem/component being analyzed.
2	FAILURE MODE NUMBER AND DESCRIPTIONS: This column describes the failure mode considered. These failure modes are generally loss of signal, incorrect signal, or short/open of critical parts. The failure mode number is crossed referenced to the drawings generated for the analysis and included in the documented report.
3	FAILURE EFFECT ON ASSEMBLY: This column identifies the effect of the postulated failure mode on the assembly under analysis.
4	FAILURE EFFECT ON SYSTEM: This column is used to record effect of the postulated failure mode on a higher assembly as defined by the analysis ground rules.
5	ITEM FAILURE PROBABILITY: This column is used to record effect of the probability of reoccurrence, such as high, medium, or low.
6	CRITICALITY CATEGORY: This column is used to record the relative severity of the failure effect using the definitions described in Table 4-1.
7	MITIGATION: This column is used to identify in-flight corrective action for mitigating the system failure effects.

Figure 4–2. Example FMEA Worksheet

4.2.2 Electrical Stress Analysis.

A detailed EEE part stress analysis shall be performed on all parts where review of the circuit indicates that individual part electrical/thermal stresses may approach the maximum allowable levels of the FAME program high reliability derating criteria specified in SSD-D-210. The derating criteria of SSD-D-210 will be used for the FAME program and the results summarized in NCST-D-FM015.

4.2.3 Worst Case Analysis.

A detailed worst-case performance analysis shall be performed on those critical flight circuits identified at PDR and listed in NCST-D-FM015. The purpose of this analysis is to verify that adequate performance margins exist for key circuit performance parameters at nominal and worst-case conditions, and to provide a basis for recommended design improvements where inadequate performance margins exist.

The analysis considers the effects of part parameter variations due to initial manufacturing tolerances (where not factored out by an acceptable trimming procedure), temperature variations end-of-life and radiation effects. Typical worst-case analyses performed will be:

- Discrete switching circuit worst-case analyses
- Digital circuit worst-case analyses
- Analog circuit worst-case analyses
- Power converter and power conditioning circuit worst-case analyses
- Optocoupler circuit worst-case analyses
- RF circuit analyses

Both manual and computer-aided analysis techniques are employed, as applicable. The worst-case analysis results are formally documented, with any questions of insufficient performance margin resolved via design review. *Worst Case Analysis and Part Derating Guidelines and Criteria*, SSD-S-210, will be followed in the performance of the FAME program worst-case analyses.

4.3 System Reliability Analysis.

As the unit and subsystem reliability analyses are developed, they will be used to update and refine the FAME program system level FMEA, NCST-D-FM011, and Single Point Failure Summary. This provides visibility for assessing further reliability improvement based upon overall FAME program considerations.

4.4 Design Reviews.

4.4.1 System Requirements Review (SRR).

A System Requirements Review (SRR) shall be held early in the program to define and document system requirements and methods used to ensure that each requirement has been met. A preliminary version of this plan and the *FAME Quality Assurance Plan*, NCST-D-FM005, will be available for review at the SRR.

4.4.2 Preliminary Design Review (PDR).

A Preliminary Design Review (PDR) shall be held early in the design phase to verify the inherent feasibility of the design concepts. Subsystems for which worst-case analysis and FMEA are to be performed will be identified during the PDR and documented in NCST-D-FM015 and NCST-D-FM011, respectively. A released version of this plan and the *FAME Quality Assurance Plan*, NCST-D-FM005, will be available for review at the PDR.

4.4.3 Critical Design Review (CDR).

A Critical Design Review (CDR) shall be held just prior to the detailed design freeze on the major hardware elements being considered and used to verify the performance, reliability and producibility of the new design elements prior to fabrication and assembly. The reliability information presented includes the final FMEA's, reliability models, and predictions to verify maximized reliability achievement. NCST-D-FM011 and NCST-D-FM015 will be revised to reflect analytical results and will be included in the CDR package. These results will also be presented at the CDR.

4.4.4 Flight Component Review (FCR).

Flight Component Reviews (FCR) shall be held for buy-off of major flight components as described in NCST-D-FM005.

4.4.5 Test Readiness Review (TRR).

A Test Readiness Review (TRR) shall be held prior to system level testing as described in NCST-D-FM005.

4.4.6 Pre-Ship Review (PSR).

A Pre-Ship Review (PSR) shall be held and serve as a system level buy-off of the integrated vehicle prior to shipment to the launch site.

4.4.7 Flight Readiness Review (FRR).

Flight Readiness Review (FRR) - Review of ground systems and flight operational documentation.

4.4.8 Additional Supporting Reviews.

Supporting design reviews shall be held, as necessary, at the subsystem levels where significant new design, modifications, and/or contractor participation is involved.

5. PARTS MATERIALS AND PROCESSES

5.1 General.

The following paragraphs provide the approach to be used for parts procurement and control for the FAME program.

5.2 Parts Selection.

NCST defines three quality levels of EEE parts procurement. These levels are based on performance and reliability requirements. These quality levels are defined as:

Level 1 - Parts shall be selected and processed to this level for programs requiring the lowest acceptable level of risk and continued performance or performance on demand is critical. These parts are selected for operational satellites with mission duration's equal to or greater than five (5) years, with functional or block redundancy, and requires Program Manager approval for single point failures.

Level 2 - Parts shall be selected and processed to this level for programs with low to moderate levels of risk balanced by cost constraints where high performance and extended life is required. These parts are selected for scientific or experimental satellites with mission duration's of one (1) to five (5) years and limited redundancy for primary objectives.

Level 3 - Parts shall be selected and processed to this level for programs with moderate levels of risk may be acceptable, and where cost is a constraint. These parts are selected for experimental satellites with mission duration's of lone (1) year or less.

Parts selected and processed for the FAME program shall be Level 2. Parts selection and guidelines shall follow the guidelines of *Instructions for EEE Parts Selection, Screening, and Qualification*, 311-INST-001. Additionally, parts selected for the program will meet the following guidelines as a minimum.

- MIL-STD-975, Grade 2 Parts List, when applicable
- MIL-STD-883, Class B Microcircuits
- JANTXV, JANTX Semiconductor Devices
- Passive devices procured under established reliability level of RSS and RRS
- Semi-custom parts such as converters procured at the Class B equipment level

Level 1 and Level 2 surplus parts, existing in NCST secured stores, may used on the FAME program.

5.3 Nonstandard Parts Approval.

The FAME Material Review Board (MRB) will review and approve all nonstandard parts prior to their incorporation into the FAME design baseline. NCST and FAME program contractor designers will submit requests for consideration on nonstandard parts using the NCST Nonstandard Parts Approval Request (NSPAR) form (see procedure MP-09.01) with the appropriate supporting documentation in accordance with SSD-D-002.

5.4 Parts Specifications.

When the FAME hardware design requires a nonstandard part, NCST or the FAME contractors will generate a custom specification patterned to the most applicable military specification or specification for the closest approved part specified in 311-INST-001. The FAME MRB will review each part specification to verify compliance prior to approval and incorporation into the revision controlled design documentation database.

5.5 Destructive Physical Analysis.

There will be no additional Destructive Physical Analysis (DPA).

5.6 Parts Stress Derating.

The electrical and thermal derating of EEE parts as specified in SSD-D-210 will be applied to the stress analysis of all FAME system elements.

5.7 Parts Radiation Hardness.

The FAME EEE parts shall be able to withstand the radiation levels as specified in the *FAME Radiation Effects Plan*, NCST-D-FMXXX.

5.8 Parts and Materials Procurement.

NCST will procure the EEE parts for the entire FAME program in a centralized approach. The parts list of each FAME subsystem, after the review and approval process, will be integrated into the *FAME EEE Parts List*, NCST-D-FM012. Likewise, all materials will be integrated into the *FAME Materials List*, NCST-D-FM013.

5.9 Parts Identification and Traceability.

Parts traceability requirements shall be as specified in the *FAME Quality Assurance Plan*, NCST-D-FM005. Part identification procedures will be established and care will be taken to isolate FAME parts from the high reliability parts screened to SSD-D-002.

5.10 Parts Problem Assessment and Reporting.

NCST participates in the Government-Industry Data Exchange Program (GIDEP) system and reviews all published alerts to assess their applicability and impact on all NCST space flight hardware including units on-orbit as well as in-process development and production activity. Should a GIDEP alert involve a part used in the FAME program, NCST will institute a documented closed loop system to ensure a timely and technically sound analysis and disposition of the application. NCST, as the centralized parts program implemented for FAME, will ensure the assessment process involves FAME program contractors. Further, NCST will generate reports for submission to the GIDEP system should part problems be identified that have potential impact to other programs.

5.11 Nonconforming Parts Dispositioning.

Nonconforming EEE parts of the FAME program will be processed in accordance with NCST procedure QA-14.01, Nonconforming Material Reports (NMRs).

5.12 Part Failure Processing.

Part failures occurring after assembly will prompt the documentation, review, analysis and disposition process detailed in NCST procedure SSD-D-008.

5.13 Processes Selection and Control.

Standard manufacturing processes and control shall be in accordance with NCST procedure MP-11.01, Development and Control of Standard Processes.

5.14 Processes Verification.

Design and process verification shall be in accordance with NCST-D-FM005 and NCST procedure CP-03.03, Configuration Item Verification.

5.15 EEE Parts and Materials Procurement Report.

The effectiveness of the parts program is largely dependent upon the instantaneous visibility of detail schedule and progress information thereby allowing sound management decisions of resource direction and control. The FAME managers will have access to current anticipated delivery dates for parts and materials and thus can identify potential fabrication schedule problems when the greatest number of alternative solutions are available. All EEE parts, materials and related issues will be contained and tracked in NCST-D-FM012 and NCST-D-FM013.

6. TESTING

The most significant element of assuring mission success is a comprehensive acceptance test and check-out program. The details of the FAME test program are documented in the *FAME Test Plan*, NCST-TP-FM001.

7. NOTES

7.1 Acronyms and Abbreviations.

Acronym	Definition
CDR	Critical Design Review
CP	Control Procedure
DPA	Destructive Physical Analysis
EEE	Electrical, Electronic and Electromechanical
FAME	Full-sky Astrometric Mapping Explorer
FCR	Flight Component Review
FMEA	Failure Modes and Effects Analysis
FRR	Flight Readiness Review
GIDEP	Government-Industry Data Exchange Program
MP	Manufacturing Procedure
MRB	Material Review Board
NCST	Naval Center for Space Technology
NMR	Nonconforming Material Report
NSPAR	Non-Standard Parts Request
PDR	Preliminary Design Review
PSR	Pre-Ship Review
SPFS	Single Point Failure Summary
SRR	System Requirements Review
TRR	Test Readiness Review